

WHAT IS CLAIMED IS:

1 1. An electronic document authenticity assurance  
2 method comprising the steps of:

3 dividing an electronic document into a plurality  
4 of constituent elements; and

5 affixing electronic signatures to all subsets of  
6 a set including the plurality of constituent elements.

1 2. An electronic document authenticity assurance  
2 method comprising the steps of:

3 dividing an electronic document into a plurality  
4 of constituent elements;

5 creating data in which information specifying a  
6 relationship between each of the plurality of  
7 constituent elements and a structure of the electronic  
8 document is bound to a respective one of the plurality  
9 of constituent elements; and

10 affixing an electronic signature to the bound  
11 data.

1 3. An electronic document authenticity assurance  
2 method comprising the steps of:

3 dividing an electronic document into a plurality  
4 of constituent elements;

5 creating data in which hash values respectively

6 calculated on the plurality of constituent elements by  
7 means of a cryptographic hash function are bound to the  
8 respective plurality of constituent elements; and  
9 affixing an electronic signature to the bound  
10 data.

1 4. An electronic document authenticity assurance  
2 method comprising the steps of:  
3 dividing an electronic document into a plurality  
4 of constituent elements;  
5 generates and binds random-numbers to the  
6 respective constituent elements;  
7 creating data in which hash values respectively  
8 calculated on the plurality of random-numbered  
9 constituent elements by means of a cryptographic hash  
10 function are bound to the respective plurality of  
11 random-numbered constituent elements; and  
12 affixing an electronic signature to the bound  
13 data.

1 5. An electronic document disclosure system  
2 comprising:  
3 an original document creator unit which divides an  
4 electronic document into a plurality of constituent  
5 elements, affixes electronic signatures to all subsets  
6 of a set including the plurality of constituent elements,

7 and stores the resultant electronic document into a  
8 document management unit;

9 a disclosure document creator unit which takes out  
10 a disclosure object document from among electronic  
11 documents stored in the document management unit, at the  
12 time of acceptance of an information disclosure request,  
13 creates a disclosure document in which information not  
14 to be disclosed is omitted from the disclosure object  
15 document, and sends the disclosure document to a  
16 recipient unit; and

17 the recipient unit which verifies a signature of  
18 an original document creator at the time of acceptance  
19 of the disclosure document which is made published.

1 6. An electronic document authenticity assurance  
2 method using a unit of a third-party organ, comprising  
3 the steps of:

4 dividing an electronic document into a plurality  
5 of constituent elements; and

6 depositing all subsets of a set including the  
7 plurality of constituent elements into the unit of the  
8 third-party organ as assurance object information.

1 7. An electronic document authenticity assurance  
2 method using a unit of a third-party organ, comprising  
3 the steps of:

4       dividing an electronic document into a plurality  
5 of constituent elements;  
6       creating data in which information specifying a  
7 relationship between each of the plurality of  
8 constituent elements and a structure of the electronic  
9 document is bound to a respective one of the plurality  
10 of constituent elements; and  
11       depositing the created data into the unit of the  
12 third-party organ as assurance object information.

1   8.   An electronic document authenticity assurance  
2 method using a unit of a third-party organ, comprising  
3 the steps of:

4       dividing an electronic document into a plurality  
5 of constituent elements;  
6       calculating hash values on the plurality of  
7 constituent elements respectively by means of a  
8 cryptographic hash function and depositing data in which  
9 the calculated hash values are bound together into the  
10 unit of the third-party organ as assurance object  
11 information.

1   9.   An electronic document authenticity assurance  
2 method comprising the steps of:

3       dividing an electronic document into a plurality  
4 of constituent elements;

5           generating random numbers for the respective  
6   plurality of constituent elements and binding the random  
7   numbers to the respective plurality of constituent  
8   elements; and  
9           calculating hash values on the respective  
10   plurality of constituent elements to which the  
11   respective random numbers are bound, by means of a  
12   cryptographic hash function; and  
13           depositing data in which the calculated hash  
14   values are bound together into a unit of a third-party  
15   organ as assurance object information.

1   10.   An   electronic   document   disclosure   system  
2   comprising:  
3           an original document creator unit which deposits  
4   assurance object information into a unit of a  
5   third-party organ with regard to a created electronic  
6   document in accordance with an electronic document  
7   authenticity assurance method using the third-party  
8   organ, according to any one of claims 6 to 9, and stores  
9   the assurance object information into a document  
10   management unit;  
11           a disclosure document creator unit which takes out  
12   a disclosure object document from among electronic  
13   documents stored in the document management unit, at the  
14   time of acceptance of an information disclosure request,

15 creates a disclosure document in which information not  
16 to be disclosed is omitted from the disclosure object  
17 document, and sends the disclosure document to a  
18 recipient unit; and

19 the recipient unit which requests the unit of the  
20 third-party organ to verify the authenticity of the  
21 disclosure document, at the time of acceptance of the  
22 disclosure document which is published.

1 11. A method which discloses an electronic document to  
2 which an electronic signature is affixed in accordance  
3 with an electronic document authenticity assurance  
4 method according to any one of claims 1 to 4, comprising  
5 the steps of:

6 designating as a disclosure object document the  
7 electronic document to which the electronic signature  
8 is affixed;

9 creating a disclosure document in which  
10 information not to be disclosed is omitted from the  
11 disclosure object document; and

12 further affixing a signature to the disclosure  
13 document.

1 12. An electronic document disclosure system  
2 according to claim 5, wherein,

3 the disclosure document creator unit affixes

4 another signature of the disclosure document creator  
5 unit to the disclosure document in which the information  
6 not to be disclosed is omitted.

1 13. An electronic document authenticity assurance  
2 method comprising the steps of:  
3       dividing an electronic document into a plurality  
4 of constituent elements;  
5       creating data indicative of undisclosure and  
6 respectively corresponding to the plurality of  
7 constituent elements;  
8       calculating signature object data related to the  
9 plurality of constituent elements, from the plurality  
10 of constituent elements and the data indicative of  
11 undisclosure and respectively corresponding to the  
12 plurality of constituent elements;  
13       binding together the calculated signature object  
14 data; and  
15       affixing an electronic signature to the bound  
16 data.

1 14. An electronic document disclosure method  
2 comprising the steps of:  
3       if first information not to be disclosed is  
4 included in constituent elements which constitute a  
5 signed electronic document created in accordance with

6 an electronic document authenticity assurance method  
7 according to claim 13, omitting constituent elements  
8 corresponding to the first information and leaving data  
9 indicative of undisclosure corresponding to the first  
10 information;

11 if second information to be disclosed and not to  
12 be made undisclosed in future is included in the  
13 constituent elements, leaving constituent elements  
14 corresponding to the second information and omitting  
15 data indicative of undisclosure corresponding to the  
16 second information; and

17 if third information to be disclosed and to be made  
18 undisclosed in future is included in the constituent  
19 elements, leaving both constituent elements and data  
20 indicative of undisclosure corresponding to the third  
21 information.

1 15. An electronic document disclosure system  
2 comprising:

3 an original document creator unit which affixes an  
4 electronic signature to a created electronic document  
5 in accordance with an electronic document authenticity  
6 assurance method according to claim 13, and stores the  
7 obtained original document into a document management  
8 unit;

9 a disclosure document creator unit which takes out



10 a disclosure object document from among electronic  
11 documents stored in the document management unit, at the  
12 time of acceptance of an information disclosure request,  
13 and creates a disclosure document in which:

14 if first information not to be disclosed is  
15 included in constituent elements included in the  
16 disclosure object document, constituent elements  
17 corresponding to the first information are omitted and  
18 data indicative of undisclosure corresponding to the  
19 first information are left;

20 if second information to be disclosed and not to  
21 be made undisclosed in future is included in the  
22 disclosure object document, constituent elements  
23 corresponding to the second information are left and  
24 data indicative of undisclosure corresponding to the  
25 second information are omitted; and

26 if third information to be disclosed and to be made  
27 undisclosed in future is included in the disclosure  
28 object document, both constituent elements and data  
29 indicative of undisclosure corresponding to the third  
30 information are left, and

31 the disclosure document is created and is sent to  
32 a recipient unit; and

33 the recipient unit which verifies the authenticity  
34 of an original document creator, at the time of  
35 acceptance of the disclosure document which is

36 published.